DOI: 10.18372/2307-9061.57.15039
УДК 347.824.2(045)

Vladimer Svanadze,
Chairman of the Board of «Internet Development Initiative IDI»,
Co-founder of «Georgian Cyber Security Academy CSA»

CYBERSECURITY IN THE CIVIL AVIATION AND EXISTING CHALLENGES

Georgian Cyber Security Academy CSA
Tbilisi, Georgia
E-mail: svanlado@gmail.com

Purpose of the article: *by this article the author wants to reveal the provisions and features regulations, structures and standards of International Organizations works in Cybersecurity in The Civil Aviation.* ***The methodological basis*** *of the research comprises general scientific and special methods.* ***Results:*** *the legislation of ICAO and ITAO is vitally crucial to ensure cybersecurity for the civil aviation. All stakeholders, in particular, public and private sectors as wells as the representatives of academia should be involved in the process of protecting critical infrastructure of the Civil Aviation.* ***Discussion:*** *cyber security in civil aviation is mainly based on the cyber technologies used to increase the safety and efficiency of air transport. At the same time, the interconnection of systems and reliance on technology is a prerequisite for the emergence of new cyber threats and risks. An interconnected computer system is widely used in the aviation industry.*

Keywords: *cybersecurity; cyberspace; Civil Aviation; cyber environment; protection of rights in cyberspace; ICAO; ITAO; ISO.*

Problem statement and its relevance. In the 21st century the process of using the Internet, Internet technologies and e-services in daily life as well as on national and industrial level is becoming more and more actual. Various industries where the management processes are partly or fully authomatised are geting more depend to modern technologies. Taking into account the current situation existing on global market and with the purpose to achieve highest possible efficiency in the working process, private sector constantly evolves and implements innovative technologies.

In fact, the development of Internet and Internet technologies still remains as huge challenge. On the other hand, accelerated process of developing Internet technologies and e-services will be a major stimulus to sophisticate the process of ensuring Internet security and stability, which will further increase the demand for this sector from both the public and private sectors, which is driven by global market demands.

Analysis of research and publications. The issue was studied using the regulations, standards and guidance of ICAO, ITAO, ISO and others organizations.

Purpose of the article. In this article the author wants to reveal the provisions and features regulations, structures and standards of International Organizations works in Cybersecurity in The Civil Aviation.

The presentation of the main material. The recent increase in the number of cyberattacks, and the sophisticated methods and means of hacking attacks, show that threats are growing at the level of both states and to individual industries. The development of Internet technologies allows us to say that cyber attacks will take more massive and sophisticated look and the increasement of the number of cybercrimes is inevitable.

In fact, technologies, e-governance services and cybersystems have become inseparable parts of modern societies where existing activities highly depend to information technologies and their evolvement. At the same time, the problem of

cybersecurity occurs and it concerns the whole critical infrastructure as well as separate systems. According to the fact that systems are globally interconnected and interdependent, cyberattacks and threats existing in cyberspace have transnational effect and character. Additionally, it affects all national actors both at national and international levels.

Exactly in this kind of cybersecurity environment operates the civil aviation which is one of the leading global industrial spere where the process of management is fully automatized. The operation and development of the above-mentioned sphere is directly proportional to the evolvement of the Internet, new technologies and e-services and it increases the risk of hacker attacks on all areas of the civil aviation. Accordingly, it is becoming more and more actual to ensure secure and stable Internet for the civil aviation with the purpose to strengthen its security.

Cyber security in civil aviation is mainly based on the cyber technologies used to increase the safety and efficiency of air transport. At the same time, the interconnection of systems and reliance on technology is a prerequisite for the emergence of new cyber threats and risks. An interconnected computer system is widely used in the aviation industry. It includes air navigation systems, aircraft control and communication systems, airport ground systems, flight information systems, security screening and many other systems used on a daily basis and for everyone. The tendency in the aviation industry is becoming increasingly digital, which poses increasingly new threats to the critical infrastructure of a given industry.

According to the need and importance of protecting critical civil aviation infrastructure, information and communication systems as well as information systems and cyber threats, in particular, ICAO is ready to develop a robust cybersecurity framework. The 40th Session of the ICAO Assembly adopted Resolution A40 - 10 "Solving Cyber Security in Civil Aviation" [1]. The resolution addresses the provision of cyber security in civil aviation with horizontal, large-scale and functional approaches. It also emphasizes the importance of protecting critical civil aviation infrastructure systems and data from cyber threats, and calls on member states to use the ICAO Cyber Security Strategy [2].

The Cyber Security Strategy for Civil Aviation was adopted by ICAO on October 4, 2019 and as we have already mentioned above it represents a recommendation document for the field of civil aviation of the member countries of the organization.

This strategy offers ICAO a conceptual vision in which the aviation industry must be resilient to cyber attacks while maintaining credibility at the global, regional and national levels. The organization also offers some points on how to achieve all this, namely:

States should recognize their obligations under the International Civil Aviation Convention (Chicago Convention [3]), which provides flight safety, aviation security and cybersecurity for continuity of civil aviation activities;

Coordination of cyber security measures between government agencies to ensure effective management of cyberspace risks;

All stakeholders which are involve in the field of civil aviation are committed to develop cyber resilience and protect against cyber attacks that may affect flight safety, aviation safety and air transport system continuity.

The strategy is relevant to other ICAO initiatives related to cybersecurity and is coordinated with relevant provisions regarding flights and aviation security management. The goals of the strategy are achieved through principles, measures and actions, which in turn are based on the following seven basic elements:

1) International cooperation – According to existing threats and risks, civil cybersecurity must be agreed at the national, regional and international levels. For this purpose, ICAO represents a world-class forum and the best platform, on the platform of which it is possible to discuss cyber security issues at the international level. To achieve this, the organization organizes various discussion meetings, seminars or other events;

2) Management – ICAO recommends all its member states to develop cybersecurity according to relevant standards [4]. Also to draw out a strictly defined national governance structure;

3) Effective legislative base and normative acts – The main purpose of international, regional and national civil aviation legislation and normative acts is to promote the implementation of a comprehensive cyber security strategy to protect against the impact of civil aviation and passenger cyber attacks;

4) Cyber Security Policy – Cybersecurity should be integrated into government aviation safety and security control systems as part of a comprehensive risk management system;

5) Exchange of the information – It is essential that appropriate mechanisms for the exchange of information be recognized in accordance with existing ICAO provisions. Given that civil aviation is a combination of interconnected systems at the global level, cyber-attacks can therefore be freely spread globally. The purpose of the information exchange is to prevent a previous incident in a timely manner;

6) Plan events and respond appropriately in the event of incidents and emergencies – Responding to incidents and taking appropriate action in emergency situations is carried out according to a pre-designed plan. Staff qualification and professional training play a very big role here;

7) Formation of the cybersecurity culture, retraining of personel and developement of the capacities – Staff should be constantly prepared and retrained. Also, it is influential to periodically raise their awareness regarding existing cyber threats and how to protect themselves from them as well as conduct cyber hygiene courses. All this, as a whole, enable the formation of cyberculture. In parallel all of the above mention, cyber security capabilities must be developed in accordance with ICAO standards.

It is noteworthy that several working groups have been set up within the ICAO to carry out their activities in the field of civil aviation cyber security, in particular: ICAO Secretariat Study Group on Cybersecurity (SSGC)

Resolution A39-19 – determines the measures to be taken by States and other stakeholders to address cyber threats existing against civil aviation, with the horizontal and joint approach. Despite of this, ICAO has been tasked with assisting and achieving the adoption of a comprehensive cybersecurity, cyber security and cybersecurity work plan and governance structure with all relevant stakeholders. To properly implement this resolution, the ICAO Secretariat Study Group on Cybersecurity (SSGC) was established in August 2017. This group is organised as plenary group which is supported by one subgroup - Research Sub - Group on Legal Aspects, and three working group - Working Group on Airlines and Aerodromes, Working Group on Air Navigation Systems and Working Group on Cybersecurity for Flight Safety.

The scope of the group is to:

a) Serve as the focal point for all ICAO cybersecurity work;

b) Define relevant areas to be considered by the Working Groups (WG) of the SSGC and validate their respective terms of reference to ensure that no overlapping of duties and responsibilities occur;

c) Conduct a review of ICAO Annexes to consolidate existing Standards and Recommended Practices (SARPs) related to cybersecurity;

d) Review the proposals for amendments to ICAO provisions or new provisions to be developed related to cybersecurity proposed by the Working Groups;

e) Encourage the development of, and participation in, government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts;

f) Promote cybersecurity awareness throughout the aviation community.

This group includes public and private sector representatives from 43 member states as well as 12 observers from international organizations.

Research Sub - Group on Legal Aspects (RSGLEG)

The purpose of creating this subgroup is to resolve cybersecurity issues against civil aviation within the framework of the necessary international legal framework.

The scopes of work to:

a) Categorize or analyze the cyber threats and vulnerabilities to civil aviation and associated risks identified by ICAO expert groups in order to establish to what extent the current legal international framework covers them;

b) Establish a common understanding and terminology of the cyber security language, including on aspects such as "cybersecurity as it relates to aviation", "computers", "unauthorized access", "vulnerabilities", "threats" and "weapons";

c) Review and analyze (in relation to the identified threats, risks and actors) the adequacy of the current international legal framework as well as assess the need to reinterpret (acknowledging that judiciary might be hesitant to do so) or amend the existing international air law instruments dealing with cyber threats legal framework or to adopt new instruments or SARPs;

d) Analyze cybersecurity related international instruments developed in other international transportation and communications domains such as maritime or railway or telecommunications in order to determine whether certain provisions could serve as analogy/a reference for the aviation international legal framework;

e) Based on the above review and analysis, identify aspects or matters that may require referral to the ICAO Legal Committee, AVSEC Panel or other ICAO bodies for further consideration and action.

Working Group on Airlines and Aerodromes (WG - AAD)

The working group implements its authority in the scope of the ICAO SSGC for the purpose to ensure cybersecurity of the airport operations. The Group's activities focus on protecting infrastructure, passengers and airline systems. The Group does not operate in the field of air navigation systems.

The objectives of the group are to:

a) Advise the SSGC on cybersecurity matters related to the airport and airline operations at aerodromes, not related to air navigation systems;

b) Coordinate development and/or updates of relevant Standards and Recommended Practices and Guidance Materials through the respective ICAO Panels and Study Groups;

c) Determine all relevant cybersecurity areas affecting airport and airline operations on the ground, not related to air navigation systems and prioritize them accordingly for action;

d) Coordinate through the SSGC, as necessary, on cross-cutting matters with other SSGC Working Groups.

The Working Group on Cybersecurity for Flight Safety (WG - CFS)

The working group aims to ensure the aspects of cybersecurity, security and cyberresilience concerns to the use of aircrafts.

The objectives of the group are to:

a) Advise the SSGC on cyber safety, security, and cyber resilience airworthiness matters;

b) Coordinate development and/or updates of relevant Standards and Recommended Practices and Guidance Materials through the respective ICAO Panels and Study Groups;

c) Determine all relevant cyber safety, security, and cyber resilience areas affecting airworthiness and prioritize them accordingly for action;

d) Coordinate through the SSGC, as necessary, on cross-cutting matters with other SSGC Working Groups.

The Working Group on Air Navigation Systems (WG - ANS)

The working group has created to resolve the aspects regarding cybersecurity, security and cyber resilience of existing and modern airports, air navigation and information management systems.

The objectives of the group are to:

a) Advise the SSGC on cyber safety, security, and cyber resilience ANS and airport operations matters for current and future environment;

b) Coordinate development and/or updates of relevant Standards and Recommended Practices Procedures and Guidance Material, as necessary, through the respective ICAO Panels and Study Groups;

c) Determine all relevant cyber safety, security, and cyber resilience areas affecting ANS, airport operations and SWIM interoperability and prioritize them accordingly for action;

d) Coordinate through the SSGC, as necessary, on cross-cutting matters with other SSGC Working Groups.

In close cooperation with ICAO, ITAO is also involved in Transportation Aviation Cyber Security [5]. In particular, the organization has a positive impact on how the industry responds to cyber security challenges. ITAO is working on a cyber security strategy, under which the organization has developed

the Aviation Cyber Security document [6]. This activity is led by the Security Advisory Council (SAC) [7], which was established in June 2019.

As we have already mentioned, ITAO cooperates with ICAO in the direction of cybersecurity. At the 40th ICAO Assembly the organization presented the Information Paper A40 - WP/395 Aviation Cyber Security – Moving Forwards [8], which outlines the need for coordinated action in the field of cyber security. In this document, ITAO expressed its support for ICAO's cybersecurity strategy [9]. Before that time, in 2018 ITAO also presented the Second High-Level Conference on Aviation Security in 2018 the Working Paper HLCAS/2-WP/27 Aircraft Digital Protection – An Integrated Approach [10]. Another influential component is the Aviation Cyber Security Roundtable (ACSR) [11]. The work of the roundtable is focused on four elements:

Cyber security culture – Promoting a positive cyber security culture and raising awareness across the industry;

Transparency and trust – Establishing a global approach to cyber security with a similar mindset to that which has guided aviation on safety and general security issues;

Communication and collaboration – Creating stronger relationships among players in the aviation industry and with external entities to improve the development of best practices and the management of potential vulnerabilities;

Workforce – Ensuring that aviation personnel are trained to recognize and manage cyber security risks; and inspire the next generation leaders.

The organization is also active in organizing cybersecurity trainings and short study courses [12].

It should be noted that the code of rules, standards and guidelines of the civil aviation cybersecurity was updated in August 2020 [13].

Normative acts implemented by ICAO and ITAO have both recommendation and compulsory character for the member states, as well as for big and average aviacompanies. It should be noted that given regulations are based on global and regional standards, in particular, standards such as ISACA, ENISA, NIST, BSI and ISO [14]. Also, it should be highlighted that there are number of communities, associations and forums created on different levels with the purpose to promote sybersecurity development in aviation industry. For instance, within the range A - ISAC, information is exchanged and analysed. It is also influential to mention about CyberSecurity Aviation SOC [15], existing on national level with the purpose to monitor, analyse and secure critical infrastructure of the aviation sector.

In **conclusion**, it should be noted that it is vitally crucial to ensure cybersecurity for the civil aviation. All stakeholders, in particular, public and private sectors as wells as the representatives of academia should be involved in the process of protecting critical infrastructure.

References

1. Assembly Resolutions in Force (as of 4 October 2019) // ICAO. 2019. URL: https://www.icao.int/ Meetings/a40/Documents/Resolutions/a40_res_prov _en.pdf.

2. Aviation Cybersecurity Strategy // ICAO. 2019. URL: https://www.icao.int/ cybersecurity/ Documents/aviation%20cybersecurity%20strategy. en.pdf.

3. Convention on international civil aviation // ICAO. 1994. URL: https://www.icao.int/ publications/Documents/7300_orig.pdf.

4. SARPs – Standards and Recommended Practices // ICAO. 2019. URL: https://www.icao.int/ safety/SafetyManagement/Pages/SARPs.aspx.

5. Our mission is to represent, lead & serve the airline industry // International Air Transport Association. 2020. URL: https://www.iata.org/.

6. Aviation Cyber Security // International Air Transport Association. 2015. URL: https://www.iata. org/contentassets/4c51b00fb25e4b60b38376a4935e2 78b/ aviation-cyber-security-position.pdf.

7. Security Advisory Council (SAC) // IATA. 2019. URL: https://www.iata.org/ en/programs/ workgroups/sac/.

8. Aviation cyber security – moving forwards // International Civil Aviation Organization. 2019. URL: https://www.icao.int/Meetings/ A40/ Documents/WP/ wp_395_en.pdf.

9. ICAO cybersecurity strategy // International Civil Aviation Organization. 2019. URL:

https://www.icao.int/Meetings/A40/Documents/WP/wp_028_en.pdf.

10. Aircraft digital protection – an integrated approach // International Civil Aviation Organization. 2018. URL: https://www.icao.int/Meetings/HLCAS2/ Documents/wp%2027%20 aircraft%20digital%20protection%20-%20an%20 integrated%20approach.pdf.

11. Aviation Cyber Security Roundtable // IATA. 2019. URL: https://www.iata.org/ contentassets/4c51b00fb25e4b60b38376a4935e278b/ sin_roundtable_readout.pdf.

12. Aviation Cyber Security (Classroom, 3 days) // IATA. 2020. URL: https://www.iata.org/en/training/courses/aviation-cyber-security/ tscs59/en/.

13. Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation // IATA. 2020. URL: https://www.iata.org/ contentassets/ 4c51b00fb25e4b60b38376a4935e278b/compilation_of_cyber_regulations_standards_and_guidance_1.0.pdf.

14. Standards, and Guidance Applicable to Civil Aviation // IATA. 2020. URL: https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation_of_cyber_regulations_standards_and_guidance_1.0.pdf.

15. Built Environment Standards // British Standards Online. 2020. URL: https://www.bsigroup.com/en-GB/standards/british-standards-online-database/building-and-construction-standards/?creative=445120693638&keyword=bsi&matchtype=b& network=g&device=c&gclid=CjwKCAjw19z6BRAYEiwAmo64LYg5SJ6XrJSyA8ZlUC6bNSabwKjqjVAmzsBc5BBEUcsU_ZgOl5KGdRoCD6EQAvD_BwE.

Владимер Сванадзе

КІБЕРБЕЗПЕКА В ЦИВІЛЬНІЙ АВІАЦІЇ ТА ІСНУЮЧІ ВИКЛИКИ

Академія кібербезпеки CSA Грузії
Тбілісі, Грузія
E-mail: svanlado@gmail.com

Метою *статті є розкриття положень та особливостей нормативних актів, стандартів та інших документів щодо діяльності міжнародних організацій у галузі кібербезпеки в царині цивільної авіації.* ***Методологічну основу*** *дослідження складають загальнонаукові та спеціальні методи.* ***Результати:*** *в ході створення наукового матеріалу автор наводить свої тези щодо базування кібербезпеки в цивільній авіації в основному на кібертехнологіях, що використовуються для підвищення безпеки та ефективності повітряного транспорту. У той же час автор наголошує на існуванні взаємозв'язку систем та опору на технології як передумову для появи нових кіберзагроз та ризиків. У авіаційній промисловості широко використовується взаємопов'язана комп'ютерна система.*

Автор зазначає, що у 21 столітті процес використання Інтернету, Інтернет-технологій та електронних послуг у повсякденному житті, а також на національному та промисловому рівні стає все більш актуальним. Різні галузі, де діють частково або повністю автоматизовані процеси управління, все більше залежать від сучасних технологій.

На думку автора дослідження, Інтернет-технології все ще залишаються величезною проблемою. Але він вказує і на те, що прискорений процес розвитку Інтернет-технологій та електронних послуг стане головним стимулом для вдосконалення процесу забезпечення Інтернет-безпеки та стабільності, що ще більше збільшить попит на цей сектор як з боку державного, так і приватного секторів, що скеровані вимогами світового ринку.

Автор детально дослідив Стратегію кібербезпеки для цивільної авіації, яка була прийнята ІКАО 4 жовтня 2019 року, і саме в ній автор вбачає рекомендаційний документ для галузі цивільної авіації країн-членів організації. Стратегія стосується різних ініціатив ІКАО, пов'язаних із кібербезпекою, і узгоджується з відповідними положеннями щодо польотів та управління авіаційною безпекою. Цілі документу досягаються за допомогою принципів, заходів та дій, які в свою чергу базуються на семи основних елементах, яким автором було приділено особливу увагу.

У висновках автор вказує на те, що нормативні джерела ІКАО та ІТАО є життєво важливим для забезпечення кібербезпеки цивільної авіації. Усі зацікавлені сторони, зокрема, державний та приватний сектори, а також представники наукових кіл повинні бути залучені до процесу захисту критичної інфраструктури цивільної авіації.

Ключові слова: *кібербезпека; кіберпростір; цивільна авіація; кіберсередовище; захист прав у кіберпросторі; ICAO; ITAO; ISO.*